WEST

Generate Collection | Print

Search Results - Record(s) 1 through 5 of 5 returned.

☐ 1. Document ID: NNRD45094

L1: Entry 1 of 5 File: TDBD Oct 1, 2001

TDB-ACC-NO: NNRD45094

DISCLOSURE TITLE: Multiple Area DataHiding Method

SECURITY: Use, copying and distribution of this data is subject to the restictions in the Agreement For IBM TDB Database and Related Computer Databases. Unpublished - all rights reserved under the Copyright Laws of the United States. Contains confidential commercial information of IBM exempt from FOIA disclosure per 5 U.S.C. 552(b)(4) and protected under the Trade Secrets Act, 18 U.S.C. 1905.

COPYRIGHT STATEMENT: The text of this article is Copyrighted (c) IBM Corporation 2001. All rights reserved.

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc

☐ 2. Document ID: NNRD42796

L1: Entry 2 of 5 File: TDBD Nov 1, 1999

TDB-ACC-NO: NNRD42796

DISCLOSURE TITLE: Watermark data-hiding for print out by printer firmware

SECURITY: Use, copying and distribution of this data is subject to the restictions in the Agreement For IBM TDB Database and Related Computer Databases. Unpublished - all rights reserved under the Copyright Laws of the United States. Contains confidential commercial information of IBM exempt from FOIA disclosure per 5 U.S.C. 552(b)(4) and protected under the Trade Secrets Act, 18 U.S.C. 1905.

COPYRIGHT STATEMENT: The text of this article is Copyrighted (c) IBM Corporation 1999. All rights reserved.

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw Desc

☐ 3. Document ID: NNRD42793

L1: Entry 3 of 5 File: TDBD Nov 1, 1999

TDB-ACC-NO: NNRD42793

DISCLOSURE TITLE: Illegal Contents Tracking by Automatic ID Embedding at Intermediate Server

SECURITY: Use, copying and distribution of this data is subject to the restictions in the Agreement For IBM TDB Database and Related Computer Databases. Unpublished - all rights reserved under the Copyright Laws of the United States. Contains confidential commercial information of IBM exempt from FOIA disclosure per 5 U.S.C. 552(b)(4) and protected under the Trade Secrets Act, 18 U.S.C. 1905.

COPYRIGHT STATEMENT: The text of this article is Copyrighted (c) IBM Corporation 1999. All rights reserved.

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | KWIC | Draw Desc

☐ 4. Document ID: NN9710177

L1: Entry 4 of 5 File: TDBD Oct 1, 1997

TDB-ACC-NO: NN9710177

DISCLOSURE TITLE: Discrimination Mechanism of Driver's License Imitations

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments KWIC | Draw Desc

☐ 5. Document ID: NN72022745

L1: Entry 5 of 5 File: TDBD Feb 1, 1972

TDB-ACC-NO: NN72022745

DISCLOSURE TITLE: Applying Safety Features and Custom Watermarks. February 1972.

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments KWIC | Draw Desc

Generate Collection Print

Terms	Documents
image and watermarks	5

Display Format: TI Change Format

Previous Page Next Page

L1: Entry 3 of 5 File: TDBD Nov 1, 1999

TDB-ACC-NO: NNRD42793

DISCLOSURE TITLE: Illegal Contents Tracking by Automatic ID Embedding at Intermediate Server

PUBLICATION-DATA:
IBM technical Disclosure Bulletin, November 1999, UK

ISSUE NUMBER: 427
PAGE NUMBER: 1516

PUBLICATION-DATE: November 1, 1999 (19991101)

CROSS REFERENCE: 0374-4353-0-427-1516

DISCLOSURE TEXT:

A program is disclosed which automatically embeds the user-ID onto the multimedia content which has been accessed from the Internet. There are many illegal multimedia contents on a open network such as the Internet which infringes the copyright of the content owner. The purpose of this program is to track not only the last illegal content user but also the whole list of illegal contents users which have passed that content.

The technology used to embed the user-ID is often referred to as digital invisible watermark. Digital invisible watermarks have the characteristic of being able to embed digital information onto digital multimedia contents without degrading the quality of the image/audio. It is required that the digital invisible watermark has the feature to continously append the user-ID watermarks to a given extent. The system may be described as the following. 1. Initially, the information which represents the copyright owner will be embedded prior to uploading into the Internet. 2. The intermediate server, e.g. provider, gateway server, proxy server, will check if there are any copyright owner information already embedded. And if there are none, the content will be downloaded as with previous methods. But if copyright owner information is already embedded, then the user-ID who requested the download will be automatically appended. A typical user-ID may be an IP address.

Previous methods of tracking illegal usage either required special hardware or had no capability of tracking previous illegal usage. A typical scenario when this program is installed on numerious intermediate servers would be the following: The first user may access the multimedia content which has the contents owner information embedded on the internet in a seemless fashion by any normal commercially available internet browser. At this point, this user will see by the browser the content which already has his/her user-ID embedded by the intermediate server but will have no problems. In a normal operation, the content will not go anywhere. But if the first user copies or captures the content and uses it on a Internet homepage the first user's user-ID is already embedded. If a second user uses this content which has the first user's user-ID embedded on a different homepage, then both the user-ID of the first user and also the second user will be embedded on the image in addition to the copyright owner information. This automatic continous user-ID appending may be repeated for a given extent. The effectiveness of this program is that when an illegal usage is found, the whole list of illegal users will be identified.

L1: Entry 1 of 5 File: TDBD Oct 1, 2001

TDB-ACC-NO: NNRD45094

DISCLOSURE TITLE: Multiple Area DataHiding Method

PUBLICATION-DATA:
IBM technical Disclosure Bulletin, October 2001, UK

ISSUE NUMBER: 450
PAGE NUMBER: 1724

PUBLICATION-DATE: October 1, 2001 (20011001)

CROSS REFERENCE: 0374-4353-0-450-1724

DISCLOSURE TEXT:

Disclosed is the technique of the Watermarking technology that allows users to embedded/retrieved multiple information to/from a single piece of digital contents. The technique consists of two parts. (1) Embedding multiple watermarks, that are not interfere to each other, into a single digital content and (2) Retrieving any but only one watermark data from the specified region in the digital content, which shows the strongest watermark signal in that specified region. The technical feasibility of this technique is confirmed by using IBM DataHiding technology for still images, but it is also applicable to audio files as well as motion pictures.

DataHiding Technology This technique uses Invisible and robust watermarking technology, that is robust against image editing such as Trimming, Compression, Rotation, etc . Watermark information is in embedding image area itself, thus, it can retrieve watermark information from editing embedding image, not need additional area information file such as frame information. DataHiding key The detection and embedding watermark keys are designed to be symmetric, the watermark detector equipped with either detection key would only be able to detect the watermark information that is embedded using the same watermark key, and ignore the rest. Therefore, only the designated watermark information will be retrieved from the image. In addition, the watermarks with different watermark keys are orthogonal to each other, and not to interfere each other. Thus watermark regions that are embedded with different watermark keys, can be overlapped. In order to detect multiple layers of watermarks, the detector will conduct simultaneous detection using multiple detection keys to seek watermark which matches the detection key. In addition, we added an interface for the user to specify location in the digital content, where the user has the most interest. The detector will conduct detection operation centered at the user-specified location, thus will retrieve the embedded watermark that is associated to that specific location. In Fig.1 example, two different watermark information, Ai and Bi, are embedded into the same host digital image using different watermark keys Ak and Bk. Watermarked area A is embedded watermark information(Ai) with Watermark key(Ak). Watermarked area B is embedded watermark information(Bi) with Watermark key(Bk). Out of Watermarked area A and B is not-embedded area, that isn t include any watermark information.

When the user points detection request at Point-1 using Ak or Bk, he can t any information, because Point-1 is on the not-embedding area. When the user points detection request at Point-2 using Ak, he can get only Ai information. At the case of Bk, he can t any information, because Point-1 is not included Watermark area B. When the user points detection request at Point-3 using Bk, he can get only Bi information. At the case of Ak, he can t any information, because Point-3 is not included Watermark area A. When the user points detection request at Point-4 using Ak and Bk, he can get both of information Ai and Bi.

In Fig.2 example, After embedding operation, green grape image is clipped and pasted the bottom of left area. In Fig 1 case, the user can t retrieve any information on Point-1. However, in this case, when the user points detection request at Point-1 using Bk, he can get Bi information. Because watermark information Bi is copied with clipped image in Watermark area B. The example of implementation is shown below;This implementation consists of the following 2 functional units: 1) Embedding unit Embedding unit is embedded hiding information to Digital contents. The following figure is operation procedure of Embedding unit.

1.1) WM Key selection This function selects watermarking key from Watermarking key Database(A). 1.2) WM area selection This function selects and clips a part of area from Digital contents(B). Clipped area will embed hiding information by WM key. 1.3) Embedding operation This function embeds hiding information(E) to Embedding area(D) by WM key(C). Then watermarked area(F) put into Contents(B). 2) Retrieving unit: Retrieving unit is retrieved hiding information from Digital contents.

The following figure is operation procedure of Retrieving unit. 1.1) WM Key selection This function selects watermarking key from Watermarking key Database(A). 1.2) WM area selection This function selects and clips a part of area from Digital contents(B). Clipped area will embed hiding information by WM key. 1.3) Embedding operation This function embeds hiding information(E) to Embedding area(D) by

WM key(C). Then watermarked area(F) put into Contents(B).